Indonesian Journal of Electrical Engineering and Computer Science
Vol. 35, No. 2, August 2024, pp. 1122~1130
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v35.i2.pp1122-1130

Ransomware attack awareness: analyzing college student awareness for effective defense

Dedy Syamsuar[1], Udsanee Pakdeetrakulwong[2], Deden Witarsyah Jacob[3], Felixius Arelta Chandra[1]
[1]Department of Information Systems, School of Information Systems, Bina Nusantara University, Jakarta, Indonesia
[2]Department of Software Engineering, Faculty of Science and Technology, Nakhon Pathom Rajabhat University, Mueang Nakhon Pathom, Thailand
[3]Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia

Article Info

Article history:

Received Feb 24, 2024
Revised Mar 13, 2024
Accepted Apr 6, 2024

Keywords:

Cybersecurity
Higher education
Protective motivation theory
Ransomware
Theory planned behavior

ABSTRACT

There are growing concerns about security as the usage of computers in academic settings continues to increase. This research aims to investigate the level of awareness among university students regarding security threats associated with ransomware. This study examines students' behaviour and preventive motivation for ransomware attacks, along with the measures taken to mitigate these security threats. The study model combines the theory of planned behaviour (TPB) and preventive motivation theory (PMT) with additional threat awareness (TA) variables. The research findings indicate a high level of awareness regarding the dangers. TA has a positive influence on other factors, as indicated by the significant t-values (perceived severity (PS)=4.479, perceived vulnerability (PV)=3.251, response efficacy (RE)=14.344, and self-efficacy (SE)=8.034). This research also demonstrates that subjective norm (SN) and affective responses (AR) have a key impact on behavioural intention (BI). Moreover, two of the preventive motivation factors, PS and PV, significantly contribute to BI, while the other two (RE and SE) did not show a significant contribution to BI.

Corresponding Author:

Dedy Syamsuar
Departement of Information Systems, School of Information System, Bina Nusantara University
Street Raya Kb. Jeruk No.27, West Jakarta, DKI Jakarta, 11530, Indonesia
Email: dedy.syamsuar@binus.ac.id

1. INTRODUCTION

In this digital era, people increasingly rely on various information technologies for their lives. For example, the internet and other technologies have extensively changed many aspects of human life in various fields. The corona virus disease 2019 (COVID-19) pandemic outbreak massively forced people to deploy and depend on information technology, and the trend has continued till today. The pandemic has successfully accelerated digitalization in many fields [1], enlarged e-commerce adoption [2], and increased automation [3]. Students or employees were no longer required to study or work on-site only, but they could do their activity anywhere as long as they were connected to the internet [4]. This habit continues to this day, where the way people do things is very much influenced and dependent on information technology (IT). Not surprisingly, information technology can simplify and delight users in carrying out most activities.

Aside from the benefits of deploying information technology, the risks are also significantly increasing. The high adoption of IT in this field is also directly proportional to the various crimes that arise [5]. Indeed, this crime has not ultimately appeared recently, but there has been a continuing increase. The report from Statista.com [6] shows a drastic spread in ransomware attacks in most countries in 2023 compared to the same period in 2022, and the education industry suffered the most. Ransomware is malware that encrypts the victim's data and holds them hostage. Victims must pay a certain amount of money so that the attackers can free the data. However, even though the victim has transferred some money in most cases, the data remains hostage [7]. In a ransomware attack, the hacker uses an important encryption algorithm to cypher the victim's data. Joseph Popp firstly created the ransomware in 1989 [8], and the first ransomware name was AIDS Trojan, where the attack was spread via a floppy disk. Recently, hackers primarily use internet communication protocols to deliver their malware, a practical and cost-effective delivery system [9]. The consequences of ransomware attacks can include temporary or endless data loss, dislocation of normal system operations, and fiscal loss [10]. Ransomware is generally classified into crypto-ransomware and locker ransomware [7]. Recent ransomware attacks could not massively launched in the late 1990s or early 2000s due to a lack of particular computers and limited internet use [8]. In 2005, a hacker released a ransomware attack (Gpcoder) that used symmetric encryption, which became snappily eased by assaying Gpcoder ransomware and generating a countermeasure. Besides malicious websites, recent ransomware can quickly spread via flash disk, email, or even by exploiting a particular protocol [11]. It can attack from many ways to encrypt all data, even the crucial data, and demand to be paid to decrypt it.

Sophos [12] reported that the education industry was the highest-level industry that received ransomware attacks compared to other industries. Academics or students in higher education utilize information technology for academic purposes such as research, online learning, communication, and organizing [13]. They also utilize it for non-academic activities such as social media, entertainment, online shopping, financial management, creativity, and staying up to date on current events. While technology has numerous advantages, students should also need to be aware of its potential risks and privacy problems. Enterprises and governments worldwide also face multitudinous ransomware-related challenges [14]. The primary challenge is the incognizance of the ruinous impact of ransomware, as numerous individuals do not realize the extent of damage that ransomware can produce [15]. The other difficulty is extreme carelessness when browsing the internet [16] since many individuals use it without taking the appropriate precautions. Eventually, ransomware adapts to technological advancements as ransomware attacks continue to evolve with the growth of technology over time [17]. The fact that ransomware assaults have untraceable origins and that bitcoins are easily used for payment supports those who pursue similar cases. Hackers may, in fact, deliberately disseminate or misuse the data to a certain degree in some circumstances if the money is not entered within the allotted time [15]. Like recently, one of the major banks in Indonesia suffered a LockBit ransomware attack, and a total of 1.5 TB was stolen and publicly published after refusing to pay the ransom. Therefore, preventive efforts must be of concern to various groups regarding the awareness of the dangers of ransomware [18]. Furthermore, the amount required for rescue has increased with the widespread spread of ransomware attacks. Organizational realities typically demand payment of about $10.000, while individuals typically pay between $300 and $700 [7]. The encryption technology employed in some ransomware attacks is so redoubtable that payment becomes necessary, or in some cases, the decision to pay or not pay is difficult among the victims [19]. There is always the fear among victims that if they pay for the rescue, they may not be able to recover their data, and they may become targets of similar attacks again in the future. Again, if every victim pays the rescue to regain their data, this felonious enterprise will continue to thrive, and more people will be affected [7].

This research investigates how higher education students know and are aware of ransomware to prevent and decrease ransomware attacks. For this purpose, we adopt the research model of integration of theory plan behavior (TPB) and protection motivation theory (PMT) [15]. First, this study references and uses the adoption or acceptance of a technology to study their behaviour. There are wide range of information system theories that can be utilized to evaluate the acceptance of or resistance to technology by either focusing on individual adoption or examining organizational adoption [20]. We adopt TPB from Ajzen [21], which has played an essential role in predicting, evaluating, or explaining individual behavior using a specific technology. The TPB regards behavior as the result of intentions and behavioral control, with intentions determined by a set of beliefs grouped into subjective norm (SN) and affective response (AR). SN emphasizes the importance of social influence in an individual's behavior, which could be from family, peers or friends. While not explicitly part of the original TPB framework [22], AR refers to the emotional reaction or feeling associated with performing a behavior. This emotional response can influence an individual's attitude toward the behavior and, consequently, their intention to engage in it. In regards of ransomware, several authors underline the importance of researching the behavioral aspect of cybersecurity [23], [24].

Secondly, since the study relates to security awareness, it also employs PMT, which provides a basis for individual awareness toward a better understanding of their perceived threat to ransomware attacks [22]. In this study, perceived severity (PS) and vulnerability (PV) are variables used to see a student's intention to use technology. PS looks at the extent to which a person believes a particular threat or risk could have serious adverse consequences. PV relates to the extent to which a person believes they are vulnerable or can be exposed to specific threats or risks. Also, additional variables can influence individual decision-making processes in PMT, self-efficacy (SE) and response efficacy (RE). SE is related to an individual's belief in his or her ability to implement preventive behavior, where the higher the level of self-efficacy, the more likely the individual will adopt preventive behavior. RE reflects an individual's confidence in reducing or preventing threats. As the predictor of the PMT variable, Bekkers *et al.* [15] suggest a threat awareness variable. They found that threat awareness played a crucial role in determining whether an individual would take action to protect themselves from potential harm. Individuals who are highly aware of threats and have strong beliefs in their ability to respond effectively are more likely to engage in proactive behaviors to mitigate risks [19]. In combination with perceived severity, perceived vulnerability, self-efficacy, and response efficacy, threat awareness can significantly impact the decision-making process and ultimately influence the effectiveness of preventive measures.

2. RESEARCH METHOD

2.1. Measurements and analysis tools

The research model of this study is shown in Figure 1. For data collection purposes, this study adapts measurement indicators from prior research to ensure content validity. There are a total of 38-item indicators used to measure both independent and dependent variables, which are adapted from several studies [15], [17], [22], [25]. Table 1 depicts the research instruments where each variable was measured using multi-item indicators. Respondents were requested to provide their demographic and background information before completing the survey, which helped to establish the sample characteristics. The survey was conducted online, and participants were asked to rate their agreement with each item on a 5-point Likert scale. The data collected was then analyzed using statistical software to determine the relationships between the variables. Overall, the use of established measurement indicators and a rigorous data collection process enhances the reliability and validity of the study findings.

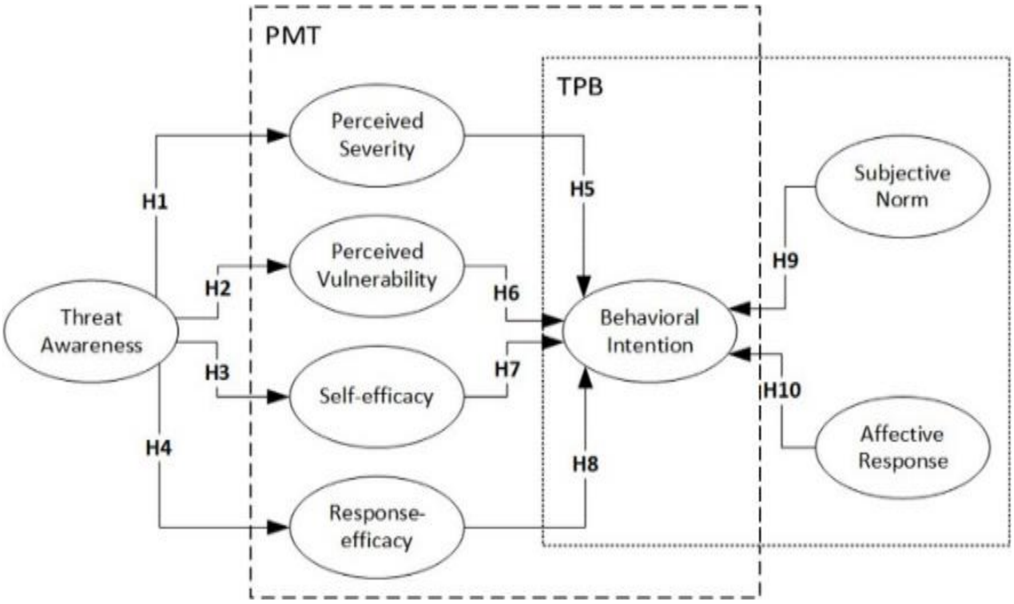

Figure 1. Research model

2.2. Respondents

This study aims to investigate higher education students' awareness of ransomware. Thus, the population of this study came from various universities that deploy internet technology to assist them in their study life. The survey was distributed to and collected from potential respondents, whether or not they were familiar with ransomware. The reason for including those who did not experience ransomware was that many of them understood the risk of the internet; however, they did not realize it was ransomware. The potential respondents were randomly selected and approached to participate in this study voluntarily. An online questionnaire was developed for data collection purposes. The links were sent directly to potential respondents or via WhatsApp's (WA) group to distribute the questionnaire. To obtain more respondents, researchers directly approached potential respondents and provided the link to the research questionnaire in the form of a QR code so the respondents could provide the answers on time.

A total of 181 students completed the questionnaire. To ensure data adequacy, we calculate the measure of sampling adequacy (MSA) [26]. The test indicated that KMO and BToS were more significant than 0.82 and 000, respectively, which the sample size was considered sufficiently large to provide adequate power [27]. Most of the respondents are between 18 and 24 years old (93.3%) from various faculties. In regards to gender, 58.6% (106) were male and 41.4% (75) were female.

3. RESULTS AND DISCUSSION

3.1. Result

There are three sub-sections in this section. First, we discussed the data preparation process to ensure the dataset is valuable and free from defects. Second, we examined the validity and reliability of the indicators, variables, and the relationship between them. Finally, we tested the hypothesis in the structural model analysis to see the relationship between variables.

3.1.1. Data preparation analysis

Data screening procedures included checking for missing values, unengaged responses, normality, and sample size [27]. Since the data was collected using an online survey, all questions were mandatory; no missing value was found. To ensure respondents seriously replied to the question, we deployed an unengaged responses test by checking the variation of answers. After the processes, the data collected descended to 168. There were 14 responses removed since respondents answered with the same score for every question. Next, Hair *et al.* [28] suggest checking distributional assumptions or normality. For this purpose, we checked every indicator's skewness and kurtosis value using WebPower [29]. The result indicated that the absolute score of all indicators was less than 3, confirming no issue with the data distribution [26].

Furthermore, we conducted the common methods bias (CMB) test. CMB may result in a systematic measurement mistake that inflates or deflates responses [30]. There are several ways to examine the CMB, including Harman's single factor, marker variable, or full collinearity test. This study adopts the third method the full collinearity test. The calculation result indicated that none of the values were higher than 5.00, indicating no issue with CMB [31]. Thus, all preparation tests indicated satisfactory results. Next, we did two stages of the statistical analysis process where the process and results will be reported in the next session.

3.1.2. Measurement model evaluation

Moving beyond data preparation, our attention shifts to the evaluation of the measurement model. The examination was conducted to determine the validity and reliability of each indicator or variable and whether they complied with the required threshold. There were a serial four stages of this assessment. First, we assessed the indicators' reliability as Hair *et al.* [27] suggested that the loading above 0.708 provided a highly recommended score. Three items were removed since each score was below the expected value (PS1, PV5, and TA5). The decision to remove items with low factor loadings underscores our commitment to ensuring that each indicator consistently measures its intended construct. Second, we assessed the internal consistency reliability to ensure the dataset was trusted by calculating the composite reliability (CR) [27], [32]. Table 1 indicates that all CR scores are higher than 0.7 and none above 0.95, confirming the reliability. The high composite reliability scores further validate the trustworthiness of our dataset, indicating a high level of internal consistency. Third, we assessed the convergent validity of each variable. This test aimed to evaluate whether or not the indicators of a particular construct converge or share a significant amount of variance. Hair *et al.* [27] suggest examining the average variance extracted (AVE), in which 0.5 or higher is considered an acceptable threshold. As presented in Table 1, the test results indicated that all AVE scores were in an acceptable threshold higher than 0.50. In the fourth stage, we focused on checking the discriminant validity, which was used to ensure that each indicator only reflects the intended variables, not other variables [28].

The initial test failed since the HTMT of Subjective norm and behavior intention value was more significant than >0.90 [28]. Therefore, a solution, as recommended by Hair *et al.* [33], was implemented to address this issue by excluding the items with a low correlation to the same construct or ones with a high connection to the opposing construct. These items were eliminated when testing revealed that BI4 showed a higher association with the opposing construct. This decisive action not only rectified the discriminant validity issue but also highlighted the importance of adaptability and rigour in the face of statistical challenges. Table 2 shows the outcomes of the HTMT test after the remedy.

Table 1. Summary of measurement model analysis

Variables	Indicators	Items	Loadings	CR	AVE
Affective response (AR)	Concerned about falling victim.	AR1	0.836	0.901	0.752
	Concerned about being harmed.	AR2	0.879		
	Concerned about potential losses.	AR3	0.885		
Behavioral intention (BI)	Taking more steps to protect.	BI1	0.866	0.919	0.790
	Learning more to prevent.	BI2	0.905		
	Willing to protect.	BI3	0.896		
Perceived severity (PS)	The attack is considerably harmful.	PS2	0.834	0.926	0.676
	The attack is considerably emotional.	PS3	0.801		
	Attacks could impact the quality of life.	PS4	0.869		
	The attack could affect the career.	PS5	0.797		
	The attack would reduce the quality of life.	PS6	0.768		
	The attack could affect financial matters.	PS7	0.859		
Perceived vulnerability (PV)	Will become infected	PV1	0.744	0.856	0.544
	Afraid of ransomware.	PV2	0.731		
	Might seriously infected.	PV3	0.723		
	Might become unusable due to.	PV4	0.708		
	Overcoming the impact.	PV6	0.779		
Response efficacy (RE)	Protecting the computer.	RE1	0.844	0.892	0.624
	Less likely to fall victim.	RE2	0.821		
	Less impacted if falling victim.	RE3	0.795		
	Having an emergency plan.	RE4	0.728		
	Knowing about the impact.	RE5	0.757		
Self-efficacy (SE)	Capable of estimating risks.	SE1	0.768	0.883	0.653
	Capable of recognizing.	SE2	0.815		
	Adequately informed about risks.	SE3	0.81		
	Preventing it by myself.	SE4	0.839		
Subjective norms (SN)	Protecting because expected.	SN1	0.858	0.862	0.758
	Influenced by friends.	SN2	0.883		
Threat awareness (TA)	Knowing how to become a victim.	TA1	0.775	0.900	0.642
	Knowing how hackers install ransomware.	TA2	0.821		
	Knowing when infected.	TA3	0.778		
	Knowing if it was secretly downloaded.	TA4	0.845		
	Having to pay to obtain files back.	TA6	0.787		

Table 2. Discriminant validity with heterrotraint-monotrait ratio (HTMT)

Variables	AR	BI	PS	PV	RE	SE	SN	TA
AR								
BI	0.726							
PS	0.693	0.449						
PV	0.623	0.573	0.660					
RE	0.162	0.474	0.290	0.255				
SE	0.142	0.330	0.207	0.248	0.731			
SN	0.654	0.899	0.598	0.579	0.847	0.630		
TA	0.271	0.458	0.354	0.359	0.836	0.557	0.809	

3.1.3. Hypothesis testing

We performed the structural model analysis using PLS with a robust foundation established through careful data preparation and measurement model evaluation. The structural model systematically examines the relationship between the variables in the research model [27] and tests whether the research hypotheses are supported. For this purpose, we run bootstrapping with sub-samples parameter=10,000 test type=one-tailed and significance level=0.05. First, we assess the path coefficient (β-value) and t-value. Which indicates how strong and direct the relationship between independent and dependent variables. The relationship between TA and PS, PV, SE and RE was positively significant with a β-value of 0.346, 0.311, 0.499, and 0.723, respectively. Also, PS and BI have a significant and negative relationship (β-value=-1.65, t-value=2.103) which indicates that consumers' desire to use technology (such as apps) decreases as they become more aware of the potential adverse effects of a ransomware infection. Both SN and AR had a significant and positive relationship to behavior intention, with a β-value of 0.465 and 0.406, respectively. However the relationship between RE or SE and BI was not significant where the path coefficients were below the minimum threshold (β-value <0.10) [26]. Table 3 presents the summary of the results of the analysis.

Next, we assessed the statistical significance of the relationship between the variables. Statistical significance is an essential concept in research as it helps determine whether the relationship between variables is likely due to chance or if it is an actual relationship. As the sample size influences the p-value, we also reported the interval confidence level (BCI-lower level and BCI-high level), which was more stable than the p-value. The results showed consistency with previous tests, as the non-significant relationship (H7 and H8) had a confidence interval between BCI-LL and BCI-UL that spanned zero. While statistical significance refers to a direction, substantive significance relates to magnitude [34]; we also examine the effect size (f^2). The result indicated that the effect size varied among the supported hypotheses, ranging from small (H5 and H6), medium (H1, H2, H9, and H10) and large (H3 and H4).

Finally, beyond individual relationships, we assessed the overall explanatory power of the model through the coefficient of determination R^2 [27]. The result indicated that TA contributed only 12% and 9.7% to PS and PV, respectively, which means TA does not affect PS and PV (<19%) [35]. However, TA contributed satisfactorily to explain 24.9% and 52.3% of the variance in SE and RE, respectively. These findings suggest that while the impact of TA on PS and PV is minimal, it plays a significant role in explaining the variance in SE and RE. The effect size for the relationship between TA and SE was moderate, while the effect size for the relationship between TA and RE was large. These results highlight the importance of threat awareness in influencing individuals' beliefs in their ability to protect themselves and their confidence in the effectiveness of their responses. The result also indicates that the value of R^2 has been particularly high, 60.6%, relative to BI.

Table 3. Summary of structural model testing

Hypotheses	Relationships	Std. beta	Std. error	t-values	P values	BCI LL	BCI UL	f^2
H1	TA→PS	0.346	0.077	4.479	p<.001	0.180	0.485	0.346
H2	TA→PV	0.311	0.096	3.251	p<.001	0.099	0.476	0.311
H4	TA→RE	0.723	0.050	14.344	p<.001	0.606	0.807	0.723
H3	TA→SE	0.499	0.062	8.034	p<.001	0.354	0.604	0.499
H5	PS→BI	-0.165	0.078	2.103	p<0.05	-0.325	-0.020	-0.165
H6	PV→BI	0.160	0.076	2.101	p<0.05	0.007	0.304	0.160
H7	RE→BI	0.069	0.076	0.906	0.365	-0.083	0.216	0.069
H8	SE→BI	-0.017	0.073	0.234	0.815	-0.165	0.124	-0.017
H9	SN→BI	0.465	0.094	4.956	p<.001	0.269	0.638	0.465
H10	AR→BI	0.406	0.087	4.674	p<.001	0.211	0.555	0.406

Note s: p<.001. p<.005 significance

3.2. Discussion

Our statistical findings are a critical phase in any research endeavor [28], offering a deeper understanding of the relationships between variables and the reliability of the data. In this discussion, we outline the intricate details discovered during the statistical analysis, including data quality and preparation, measurement model evaluation, discriminant validity, structural model analysis and the overall implications of the findings. The findings indicate that eight hypotheses are supported and two are not. Our exploration of statistical findings would be incomplete without contextualizing them within the broader landscape of existing literature. Drawing comparisons with prior studies, we excavated similarities and differences enriching the discourse on the relationships between variables in our specific context. This interplay between our findings and existing knowledge serves to refine and expand our understanding.

Regarding TA's function as a predictor, all hypotheses show a substantial correlation with different degrees of significance for each dependent variable. The results align with earlier research [15], [16] showing that students are more aware of cybersecurity concerns and more motivated to defend themselves against ransomware attacks. The results indicate that individuals with a heightened awareness of the potential risks of employing information technology resources are more ready to see the threat as significant. Consequently, when the awareness of ransomware increases, the likelihood of individuals or organizations perceiving the threat as significant and risky increases. Recognition of potential dangers can elicit emotional responses [23], such as anxiety or fear, which allows students to increase their seriousness in anticipating the threat. Those who possess genuine awareness of the situation are more inclined to use emotional elements when evaluating the gravity of the threat [36]. Moreover, having prior exposure to ransomware attacks or familiarity with prominent instances can enhance the connection between awareness of threats and the perceived level of severity [16]. These stories can provide clear and powerful lessons about the potential consequences of attacks.

Moreovers, individuals with a strong perception of severity are more ready to engage in proactive measures [14], such as strengthening their accounts, employing supplementary encryption, or doing regular backups. As the study finding indicates a strong relationship between TA and RE (R^2=52.3%), therefore it can be translated that those who have personally experienced a ransomware attack or know someone who may have a heightened perception of the seriousness of the threat. The action is because they have witnessed firsthand the potential consequences, such as loss of essential files or financial losses. Additionally, individuals who are familiar with prominent instances of ransomware attacks, such as the WannaCry attack in 2017, may be more likely to perceive the threat as significant and risky due to the widespread media coverage and the visible impact on organizations and individuals.

Another notable discovery is the link between PS and BI. In this study, the association is significant, but the direction is unfavorable. It suggests that the more students believe technology is a more severe risk, the less likely they are to use it (β-value -0.165). The result is absolutely reasonable; individuals who have appropriate awareness of cybersecurity risks will be alert, and given the risks of technology, they will construct protection against it. This finding also indicates that higher education students are aware of the importance of cybersecurity and its potential consequences. It is encouraging to see that they are taking proactive measures to protect themselves and their data from potential threats. This awareness and intention to protect themselves bodes well for their future as they enter the workforce and become increasingly reliant on technology. It also highlights the importance of continued education and awareness campaigns to ensure that individuals of all backgrounds are equipped with the necessary knowledge and skills to navigate the digital landscape safely.

Both subjective norms and affective responses indicate a significant and positive relationship. This finding is consistent with prior studies [15], [17], [22], suggesting that individuals are more likely to engage in behaviors that are influenced by social norms and emotional reactions when it comes to protecting themselves from ransomware threats. The students were more likely to adhere to cybersecurity best practices when they perceived a solid social expectation from their peers (subjective norms) and when they experienced fear or anxiety towards the consequences of a ransomware attack (affective responses).

4. CONCLUSION

Our statistical findings carry profound implications for both academic and practical domains. The careful journey through data preparation, measurement model evaluation, and structural model analysis has provided a nuanced understanding of the relationships between variables. The insights gained from our analysis contribute not only to the academic discourse but also offer practical applications in real-world scenarios. Since many activities rely on cyber technology, people have to elevate their security awareness to a high level. Cybersecurity is not only about technical aspects; behavioral properties have also become an essential area to be explored. Such ransomware attacks are more because of human behavior that invites cybercrime unintentionally. The study confirmed that the integrated model of TPB and PMT was worthwhile to cybersecurity, more specific to the ransomware context. From a practical perspective, this study provides a valuable input for competent party to prevent becoming a victim of ransomware attacks.

Some limitations of our study need to be addressed and considered for future research. First, the respondents who participated in this study and the total response were limited. Therefore, future studies need to expand the research sample and conduct a group analysis to obtain a more specific perspective of insight into the awareness motivation to protect themselves from cybercrime. Secondly, the study focused solely on ransomware, so future research should explore other types of cyber threats to gain a more comprehensive understanding of cybersecurity behavior. Overall, while our study provides valuable insights, there is still much more to be explored in this area.

ACKNOWLEDGEMENTS

This research is part of the grant PIB of the Year 2024, supported by the Bina Nusantara University and the Nakhon Pathom Rajabhat University. This research grant contract number was No: 069C/VRRTT/III/2024 on March 18, 2024.

REFERENCES

[1] L. Grinin, A. Grinin, and A. Korotayev, “COVID-19 pandemic as a trigger for the acceleration of the cybernetic revolution, transition from e-government to e-state, and change in social relations,” *Technological Forecasting and Social Change,* vol. 175, p. 121348, 2022, doi: 10.1016/j.techfore.2021.121348.

[2] M. B. Hossain, T. Wicaksono, K. M. Nor, A. Dunay, and C. B. Illes, “E-commerce adoption of small and medium-sized enterprises during COVID-19 pandemic: Evidence from South Asian Countries,” *The Journal of Asian Finance, Economics and Business,* vol. 9, pp. 291-298, 2022, doi: 10.13106/jafeb.2022.vol9.no1.0291.

[3] P. K. Kollu *et al.*, “Development of advanced artificial intelligence and IoT automation in the crisis of COVID-19 detection,” *Journal of Healthcare Engineering,* vol. 2022, 2022, doi: 10.1155/2022/1987917.

[4] I. R. Sulistiani, P. Setyosari, C. Sa’dijah, and H. Praherdhiono, “Technology integration through acceptance of e-learning among preservice teachers,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* vol. 31, pp. 1821-1828, 2023, doi: 10.11591/ijeecs.v31.i3.pp1821-1828.

[5] I. Syamsuddin and D. Syamsuar, "Live memory forensics investigations: a comparative analysis," *Journal of Advances in Information Technology*, vol. 14, 2023, doi: 10.12720/jait.14.5.950-959.
[6] Statista.com. (2023, 05 August). *Share of organizations worldwide hit by ransomware attacks in 2022 and 2023, by country*. Available: https://www.statista.com/statistics/1246438/ransomware-attacks-by-country/
[7] M. Humayun, N. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: Evolution, mitigation and prevention," *Egyptian Informatics Journal*, vol. 22, pp. 105-117, 2021, doi: 10.1016/j.eij.2020.05.003.
[8] P. O'Kane, S. Sezer, and D. Carlin, "Evolution of ransomware," *Iet Networks*, vol. 7, pp. 321-327, 2018, doi: 10.1049/iet-net.2017.0207.
[9] R. Greenlaw and K. Mufeti, "Reducing cyber crime in africa through education," in *2022 IEEE IFEES World Engineering Education Forum - Global Engineering Deans Council, WEEF-GEDC 2022 - Conference Proceedings*, 2022, doi: 10.1109/WEEF-GEDC54384.2022.9996274.
[10] A. Greubel, D. Andres, and M. Hennecke, "Analyzing reporting on ransomware incidents: a case study," *Social Sciences*, vol. 12, 2023, doi: 10.3390/socsci12050265.
[11] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "WannaCry ransomware: analysis of infection, persistence, recovery prevention and propagation mechanisms," *Journal of Telecommunications and Information Technology*, pp. 113-124, 2019, doi: 10.26636/jtit.2019.130218.
[12] Sophos.com. (2023, August 8th). *The State of Ransomware 2023*. Available: https://www.sophos.com/en-us/content/state-of-ransomware
[13] R. Fiati, W. Widowati, and S. Nugraheni, "Service quality model analysis on the acceptance of information system users' behavior," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 30, pp. 444-450, 2023, doi: 10.11591/ijeecs.v30.i1.pp444-450.
[14] J. W. Han, O. J. Hoe, J. S. Wing, and S. N. Brohi, "A conceptual security approach with awareness strategy and implementation policy to eliminate ransomware," in *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence*, 2017, pp. 222-226, doi: 10.1145/3168390.3168398.
[15] L. Bekkers, S. van't Hoff-de Goede, E. Misana-ter Huurne, Y. van Houten, R. Spithoven, and E. R. Leukfeldt, "Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model," *Computers and Security*, vol. 127, p. 103099, 2023, doi: 10.1016/j.cose.2023.103099.
[16] L. De Kimpe, M. Walrave, P. Verdegem, and K. Ponnet, "What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context," *Behaviour and Information Technology*, vol. 41, pp. 1796-1808, 2022, doi: 10.1080/0144929X.2021.1905066.
[17] J. Ophoff and M. Lakay, "Mitigating the ransomware threat: a protection motivation theory approach," in *Information Security*, M. Loock and M. Coetzee, Eds., ed: Springer International Publishing, 2019, pp. 163-175, doi: 10.1007/978-3-030-11407-7_12.
[18] A. Moallem, "Cyber security awareness among college students," in *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity*, 2019, pp. 79-87, doi: 10.1007/978-3-319-94782-2_8.
[19] S. Mujeye, "Ransomware: To pay or not to pay? the results of what IT professionals recommend," *presented at the Proceedings of the 2022 5th International Conference on Software Engineering and Information Management,* Yokohama, Japan, 2022, doi: 10.1145/3520084.3520096.
[20] D. Syamsuar, P. Dell, D. Witarsyah, and A. Luthfi, "Organizational resistance to technology diffusion: the case of IPv6," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 12, pp. 2462-2468, 2022, doi: 10.18517/ijaseit.12.6.16073.
[21] I. Ajzen, *From intentions to actions: A theory of planned behavior*. Springer Berlin Heidelberg: Springer, 1985.
[22] E. Kim and Y. Kyung, "Factors affecting the adoption intention of new electronic authentication services: a convergent model approach of VAM, PMT, and TPB," *IEEE Access*, vol. 11, pp. 13859-13876, 2023, doi: 10.1109/ACCESS.2023.3243183.
[23] R. A. M. Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, "Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity*, vol. 3, pp. 1-18, 2020, doi: 10.1186/s42400-020-00050-w.
[24] M. O. Baseskioglu and A. Tepecik, "Cybersecurity, computer networks phishing, malware, ransomware, and social engineering anti-piracy reviews," in *HORA 2021 - 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings*, 2021, doi: 10.1109/HORA52670.2021.9461272.
[25] D. Syamsuar *et al.*, "Exploring ERP user behaviour in developing countries: integrating self-efficacy and UTAUT perspectives," in *2023 ICADEIS*, 2023, pp. 1-6, doi: 10.1109/ICADEIS58666.2023.10270956.
[26] J. F. Hair, W. Black, B. Babin, and R. Anderson, *Multivariate data analysis*, 8th ed. Australia: Cengage Learning EMEA, 2019.
[27] J. Hair, G. T. Hult, C. Ringle, M. Sarstedt, N. Danks, and S. Ray, *Partial least squares structural equation modeling (PLS-SEM) using R: A workbook*: Springer Cham, 2021.
[28] J. Hair, J. Risher, M. Sarstedt, and C. Ringle, "When to use and how to report the results of PLS-SEM," *European Business Review*, vol. 31, pp. 2-24, 2019, doi: 10.1108/EBR-11-2018-0203.
[29] D. Wulandari, S. Sutrisno, and M. B. Nirwana, "Mardia's skewness and kurtosis for assessing normality assumption in multivariate regression," *Enthusiastic: International Journal of Applied Statistics and Data Science*, pp. 1-6, 2021, doi: 10.20885/enthusiastic.vol1.iss1.art1.
[30] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: a critical review of the literature and recommended remedies," *Journal of applied psychology*, vol. 88, p. 879, 2003, https://psycnet.apa.org/doiLanding?doi=10.1037%2F0021-9010.88.5.879.
[31] N. Kock, "Common method bias in PLS-SEM: a full collinearity assessment approach," *International Journal of e-Collaboration (ijec)*, vol. 11, pp. 1-10, 2015, doi: 10.4018/ijec.2015100101.
[32] D. Syamsuar and C. Darren, "Integrating trust and risk perception into UTAUT: study about consumers' purchase intentions in social media," in *2023 International Conference on Informatics, Multimedia, Cyber and Informations System (ICIMCIS)*, 2023, pp. 55-60, doi: 10.1109/ICIMCIS60089.2023.10349044.
[33] J. Hair, C. L. Hollingsworth, A. B. Randolph, and A. Y. L. Chong, "An updated and expanded assessment of PLS-SEM in information systems research," *Industrial Management and Data Systems*, vol. 117, pp. 442-458, 2017, doi: 10.1108/IMDS-04-2016-0130.
[34] J. Cohen, *Statistical power analysis for the behavioral sciences*. New york: Lawrence Erlbaum Associates, 2013.
[35] W. W. Chin, "How to write up and report PLS analyses," in *Handbook of partial least squares: Concepts, methods and applications*, ed: Springer, 2009, pp. 655-690, doi: 10.1007/978-3-540-32827-8_29.

[36] I. Shammugam, G. N. Samy, P. Magalingam, N. Maarop, S. Perumal, and B. Shanmugam, "Information security threats encountered by Malaysian public sector data centers," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 21, pp. 1820-1829, 2021, doi: 10.11591/ijeecs.v21.i3.pp1820-1829.

BIOGRAPHIES OF AUTHORS

Dedy Syamsuar, Ph.D. currently works as a lecturer in information systems at the University of Bina Nusantara in Indonesia. He completed both master's and doctoral degrees in Information Systems from Curtin University of Technology. Australia. His primary research interests include behavior to information technology to understand individual or group behavior related to the use, adoption and interaction with a wide range of information technologies. Besides that, he is also involved in joint research in IT Risk, e-Government, system development, IT security. He can be contacted at email: dedy.syamsuar@binus.ac.id.

Udsanee Pakdeetrakulwong, Ph.D. is currently an Assistant Professor at the Software Engineering Department, Faculty of Science and Technology, Nakhon Pathom Rajabhat University. She completed her Master of Science in Information Technology at Rochester Institute of Technology, New York, USA. She received a Ph.D. in Information Systems from Curtin University, Australia. She received an Ernst Mach Grant ASEA-UNINET scholarship for carrying out the post-doctoral research in St. Pölten University of Applied Sciences, Austria. Her primary research interests include semantic web technology, software engineering, blockchain technology. She can be contacted at email: udsanee@webmail.npru.ac.th.

Deden Witarsyah Jacob, ST. M.Eng. Ph.D. currently works at the School of Industrial and System Engineering. Telkom University. He finished his master's in Electrical and Computer Engineering at Curtin University of Technology, Australia. Deden continued his education for a doctoral degree in Twente University Netherlands and Universiti Tun Hussein Onn Malaysia. He joined the Cybernetics Research Group and has been Head of the Open Data Research Center since 2018 until Present. Deden also responsible for Ph.D. External Examiner to the Delf University of Technology Netherlands and PIC Coil Project with DAAD Germany. He can be contacted at email: dedenw@telkomuniversity.ac.id.

Felixius Arelta Chandra was born in Bukittinggi on September 26, 2002. Felix is a college student at Binus University in Indonesia. He attends the information system studies programme. He has a motto: believe in yourself, and you can do everything you set your mind to. Furthermore, Felix works part-time as a programmer, developing web-based or mobile apps. He can be contacted at email: felixius.chandra@binus.ac.id.